UNITED STATES DEPARTMENT OF COMMERCE
Patent and Trademark Office
Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231

√o

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.
08/883,636	06/26/97	GONG L	3070-004

LM02/0128

MCDERMOTT WILL & EMERY
600 13TH ST NW
WASHINGTON DC 20005-3096

EXAMINER	
MEISLAHN, D	
ART UNIT	**PAPER NUMBER**
2767	11

DATE MAILED: 01/28/00

Please find below and/or attached an Office communication concerning this application or proceeding.

Commissioner of Patents and Trademarks

Office Action Summary

Application No. 08/883,636	Applicant(s) Gong	
Examiner Douglas Meislahn	Group Art Unit 2767	

☒ Responsive to communication(s) filed on *Nov 24, 1999*

☒ This action is **FINAL.**

☐ Since this application is in condition for allowance except for formal matters, **prosecution as to the merits is closed** in accordance with the practice under *Ex parte Quayle* 1935 C.D. 11; 453 O.G. 213.

A shortened statutory period for response to this action is set to expire *3* month(s), or thirty days, whichever is longer, from the mailing date of this communication. Failure to respond within the period for response will cause the application to become abandoned. (35 U.S.C. § 133). Extensions of time may be obtained under the provisions of 37 CFR 1.136(a).

Disposition of Claim

☒ Claim(s) *1-8 and 13-19* is/are pending in the applicat

Of the above, claim(s) ______ is/are withdrawn from consideration

☐ Claim(s) ______ is/are allowed.

☒ Claim(s) *1-8 and 13-19* is/are rejected.

☐ Claim(s) ______ is/are objected to.

☐ Claims ______ are subject to restriction or election requirement.

Application Papers

☐ See the attached Notice of Draftsperson's Patent Drawing Review, PTO-948.

☐ The drawing(s) filed on ______ is/are objected to by the Examiner.

☐ The proposed drawing correction, filed on ______ is ☐ approved ☐ disapproved.

☐ The specification is objected to by the Examiner.

☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. § 119

☐ Acknowledgement is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d).

☐ All ☐ Some* ☒ None of the CERTIFIED copies of the priority documents have been

☐ received.

☐ received in Application No. (Series Code/Serial Number) ______ .

☐ received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

*Certified copies not received: ______

☐ Acknowledgement is made of a claim for domestic priority under 35 U.S.C. § 119(e).

Attachment(s)

☐ Notice of References Cited, PTO-892

☒ Information Disclosure Statement(s), PTO-1449, Paper No(s). 8

☐ Interview Summary, PTO-413

☐ Notice of Draftsperson's Patent Drawing Review, PTO-948

☐ Notice of Informal Patent Application, PTO-152

--- SEE OFFICE ACTION ON THE FOLLOWING PAGES ---

DETAILED ACTION

Response to Amendment

1. This action is in response to the amendment filed 24 November 1999 that cancelled claims 9-12 and amended claims 1, 3, 5, 7, 13, 15, 17, and 18.

Response to Arguments

2. Applicant's arguments filed 24 November 1999 have been fully considered but they are not persuasive. The basic tenor of the arguments is that the cited references do not show the automatic encryption of data as it is written to the data stream. Although this might well be true, language supporting this limitation had no previously been present in the claims. Finkelstein et al. (5319712) or Zuquete et al. ("Transparent Authentication and Confidentiality for Stream Sockets") read on this new limitation.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1, 2, 5, 6, 13, and 14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gillon et al. US Patent #5,838,927 in view of Elgamal et al. US Patent #5,657,390 Shaffer et al. US Patent #5,784,461 and either Finkelstein et al. (5319712) or Zuquete et al. ("Transparent Authentication and Confidentiality for Stream Sockets").

As per claims 1, 5, and 13, Gillon et al teaches a method for, computer-readable medium having stored thereon a plurality of sequences of instructions for, and a computer data signal embodied in a carrier wave representing sequences of instruction for, providing communication protocol-independent security for data transmitted between a first process, executing on a first network node, and a second process, executing on a second network node, wherein the first network node and the second network node each support at least one common communication protocol, the method comprising the steps of, the computer-readable medium having stored thereon a plurality of sequences of instructions causing a processor to perform the steps of, and the computer data signal embodied in a carrier wave representing sequences of instruction providing communication protocol independent security by performing the steps of:

establishing a first stream between the first process and the network connection (see figure 5, column 7 lines 11-15, Gillon et al.'s write stream);

establishing a second stream between the second process and the network connection (see figure 5, column 7 lines 11-15, the reception of the write stream by the client) ;

encrypting data to be transmitted between the first and second processes, the encrypting of the data being independent of the at least one communication protocol (see column 4, lines 11-14, the use of HyperText Transport Protocol) supported by the first node (see column 5, lines 60-67 and column 7 lines 4-15, Gillon et al.'s encryption of data with no header, and hence, no protocol specific information, at the stream level);

writing data to the first stream (see figure 6, element 610 and column 7 lines 9-13, Gillon et al.'s attachment of encryption and compression streams to the write stream);

causing the encrypted data to be transmitted from the first network node to the second network node (see figure 6, elements 610 and 614 and column 7 lines 13- 15, Gillon et al.'s transmission of write stream to the client);

reading the encrypted data from the second stream and decrypting the encrypted data to obtain decrypted data which is identical to the data on the first network node before it was encrypted (see figure 5 and column 6 lines 38-46, Gillon et al.'s reception and decryption of the encrypted data);

However, Gillon et al does not explicitly teach either the establishment of a communications channel, secure or otherwise, prior to the transfer of stream data or automatically encrypting data as it is written to the data stream.

Elgamal et al teaches the establishment of a secure communications channel between a first and second network node (see column 7, lines 4-8, his establishment of a secure channel by checking connection integrity and authenticating the connected parties.)

In lines 31-38 of column 5, Shaffer et al. disclose a method of encrypting data that is independent of any protocols used to establish a telecommunication data transfer connection.

In their abstract, Finkelstein et al. talk about encrypting, prior to transmission, data packets.

In their second paragraph, Zuquete et al. say that most Internet traffic is unencrypted, which is a negative. They thus propose a subsystem that provides secure channels that use end-to-end encryption.

Therefore it would have been obvious to one of ordinary skill in the computer art at the time the invention was made to combine the protocol independent encrypted system of Shaffer et al. with the stream of Gillon et al and the secure communication channel of Elgamal et al in order to improve the reliability of the data transmitted by Gillon et al's invention and thus reduce data latency experienced by the receiving node because Gillon et al suggests that latency is undesirable (column 2, lines 12-18). It would further have been obvious to encrypt data just before it is transmitted as taught by Finkelstein et al. or Zuquete et al.

As per claims 2, 6, and 14, Gillon et al does not explicitly teach the additional steps of performing a communication protocol-specific encryption of the data on the first network node and performing a communication protocol-specific decryption of the data on the second network node.

Elgamal et al teaches the steps of performing a communication protocol-specific encryption of the data on the first network node and performing a communication protocol-specific decryption of the data on the second network node (see figure 12c, and column 6 lines 10-35, Elgamal et al.'s secure sockets layer encryption of data at the server and his secure sockets layer decryption of data at the client) .

It would have been obvious to one of ordinary skill in the computer art at the time the invention was made to combine the protocol independent encryption of Gillon et al with the protocol dependent encryption of Elgamal et al in order to hide sensitive information about the source of the encrypted data and provide double encryption for the data itself because stronger encryption is universally recognized as desirable.

5. Claims 3, 4, 7, 8, 15 and 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gillon et al. US Patent #5,838,927 in view of Elgamal et al. US Patent #5,657,390 Shaffer et al. US Patent #5,784,461 and either Finkelstein et al. (5319712) or Zuquete et al. ("Transparent Authentication and Confidentiality for Stream Sockets") as applied to claims 1, 5, and 13 above, and further in view of van Hoff et al US Patent #5,761,421.

As per claims 3, 7, and 15, Gillon et al does not explicitly teach that the data streams are Java streams and Elgamal et al does not explicitly teach that the secure channel is a Java secure channel.

van Hoff et al teaches the secure transfer of Java data between two Java applets running on two clients in a network environment (see column 4 lines 26-54, van Hoff et al.'s establishment of a secure communications channel between two applets).

It would have been obvious to one of ordinary skill in the computer art at the time the invention was made to combine the streaming encryption of Gillon et al, the protocol independence of Shaffer et al., and the secure channel of Elgamal et al with the Java communications channel and Java transfer of van Hoff et al in order to allow for the encryption and secure stream transmission of Java data and objects because the maintenance of data integrity and reliability of all data types is universally recognized as desirable.

As per claims 4, 8, and 16, Gillon et al teaches the attachment of a third stream to the communication channel and the transmission of data according a specific protocol (see figure 6 element 608, column 4 lines 11-14, column 6 lines 18-23, Gillon et al.'s attachment of multiple function streams to the write stream and the use of HyperText Transfer Protocol) Official Notice is taken that multicasting and the branching of a single stream into multiple streams is old and well known in the computer art. It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the function providing streams and specific communication protocol of Gillon et al with the old and well known practice of multicasting in order to allow the fast and efficient distribution of stream data according to a specific communication protocol because high transmission speed and reduced data latency are seen as desirable in the computer art. (Gillon et al suggests that latency is undesirable (column 2, lines 12-18))

6. Claim 17 is rejected under 35 U.S.C. 103(a) as being unpatentable over Gillon et al. US Patent #5,838,927 in view of Elgamal et al. US Patent #5,657,390 Shaffer et al. US Patent #5,784,461 and either Finkelstein et al. (5319712) or Zuquete et al. ("Transparent Authentication and Confidentiality for Stream Sockets").

Gillon et al teaches a method for providing communication protocol-independent security for data transmitted by a process executing on a network node, the method comprising the steps of:

establishing a stream between the first process and the network connection (see figure 5, column 7 lines 11-15, Gillon et al.'s write stream);

encrypting data to be transmitted by processes, the encrypting of the data being independent of a communication protocol (see column 4, lines 11-14, the use of HyperText Transport Protocol) supported by the network node (see column 5, lines 60-67 and column 7 lines 4-15, his encryption of data with no header, and hence, no protocol specific information, at the stream level);

writing the encrypted data to the stream (see figure 6, element 610 and column 7 lines 9-13, Gillon et al.'s attachment of encryption and compression streams to the write stream); and

causing the encrypted data to be transmitted from a network node to another network node (see figure 6, elements 610 and 614 and column 7 lines 13- 15, Gillon et al.'s transmission of write stream to the client);

However, Gillon et al does not explicitly teach either the establishment of a communications channel, secure or otherwise, prior to the transfer of stream data or automatically encrypting data as it is written to the data stream.

Elgamal teaches the establishment of a secure communications channel between a first and second network node (see column 7, lines 4-8, Elgamal et al.'s establishment of a secure channel by checking connection integrity and authenticating the connected parties)

In lines 31-38 of column 5, Shaffer et al. disclose a method of encrypting data that is independent of any protocols used to establish a telecommunication data transfer connection.

In their abstract, Finkelstein et al. talk about encrypting, prior to transmission, data packets.

In their second paragraph, Zuquete et al. say that most Internet traffic is unencrypted, which is a negative. They thus propose a subsystem that provides secure channels that use end-to-end encryption.

It would have been obvious to one of ordinary skill in the computer art at the time the invention was made to combine the stream of Gillon et al with the secure communication channel of Elgamal et al and the protocol independent encryption of

Shaffer et al. in order to improve the reliability of the data transmitted by Gillon et al's invention and thus reduce data latency experienced by the receiving node because Gillon et al suggests that latency is undesirable (column 2, lines 12-18). It would further have been obvious to encrypt data just before it is transmitted as taught by Finkelstein et al. or Zuquete et al.

7. Claims 18 and 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gillon et al. US Patent #5,838,927 in view of Elgamal et al. US Patent #5,657,390 Shaffer et al. US Patent #5,784,461 and either Finkelstein et al. (5319712) or Zuquete et al. ("Transparent Authentication and Confidentiality for Stream Sockets") as applied to claim 17 above, and further in view of van Hoff et al US Patent #5,761,421.

As per claim 18, Gillon et al does not explicitly teach that the data streams are Java streams and Elgamal et al does not explicitly teach that the secure channel is a Java secure channel.

van Hoff et al teaches the secure transfer of Java data between two Java applets running on two clients in a network environment (see column 4 lines 26-54, van Hoff et al.'s establishment of a secure communications channel between two applets).

It would have been obvious to one of ordinary skill in the computer art at the time the invention was made to combine the streaming protocol independent encryption of Gillon et al and the secure channel of Elgamal et al with the Java communications channel and Java transfer of van Hoff et al in order to allow for the encryption and secure stream transmission of Java data and objects because the maintenance of data integrity and reliability of all data types is universally recognized as desirable.

As per claim 19, Gillon et al teaches the attachment of a second stream to the communication channel and the transmission of data according a specific protocol (see figure 6 element 608, column 4 lines 11-14, column 6 lines 18-23, Gillon et al.'s attachment of multiple function streams to the write stream and the use of HyperText Transfer Protocol) Official Notice is taken that multicasting and the branching of a single stream into multiple streams is old and well known in the computer art.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the function providing streams and specific communication protocol of Gillon et al with the old and well known practice of multicasting in order to allow the fast and efficient distribution of stream data according to a specific communication protocol because high transmission speed and reduced data latency are seen as desirable in the computer art. (Gillon et al. suggests that latency is undesirable in column 2, lines 12-18.)

Conclusion

8. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Douglas J Meislahn whose telephone number is (703) 305-1338. The examiner can normally be reached between 9AM and 6PM, except for every other Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Tod Swann can be reached on (703) 308-7791. The fax phone numbers for the organization where this application or proceeding is assigned are (703) 308-9051 for regular communications and (703) 308-9052 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.

Douglas J Meislahn
Examiner
Art Unit 2767

DJM
DJM
January 20, 2000

TOD R. SWANN
SUPERVISORY PATENT EXAMINER
GROUP 2700